VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Absolvování individuální odborné praxe

Individual professional practice in the company

2016

Václav Štrbák

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Zadání bakalářské práce

Student: **Václav Štrbák**

Studijní program: B2647 Informační a komunikační technologie

Studijní obor: 2601R013 Telekomunikační technika

Téma: Absolvování individuální odborné praxe
Individual Professional Practice in the Company

Jazyk vypracování: čeština

Zásady pro vypracování:

1. Student vykoná individuální praxi ve firmě: Orchard Hotel a.s. - Park Inn by Radisson Hotel Ostrava
2. Struktura závěrečné zprávy:
a. Popis odborného zaměření firmy, u které student vykonal odbornou praxi a popis pracovního zařazení studenta
b. Seznam úkolů zadaných studentovi v průběhu odborné praxe s vyjádřením jejich časové náročnosti
c. Zvolený postup řešení zadaných úkolů
d. Teoretické a praktické znalosti a dovednosti získané v průběhu studia uplatněné studentem v průběhu odborné praxe
e. Znalosti či dovednosti scházející studentovi v průběhu odborné praxe
f. Dosažené výsledky v průběhu odborné praxe a její celkové zhodnocení

Seznam doporučené odborné literatury:

Podle pokynů konzultanta, který vedl odbornou praxi studenta

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **Ing. Zdeňka Chmelíková, Ph.D.**

Konzultant bakalářské práce: Ing. Václav Hrstka

Datum zadání: 01.09.2015

Datum odevzdání: 29.04.2016

VYSOKÁ ŠKOLA BÁŇSKÁ - TECHNICKÁ UNIVERZITA OSTRAVA
Fakulta elektrotechniky a informatiky
OSTRAVA

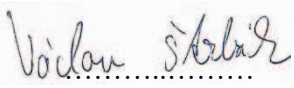
doc. Ing. Miroslav Vozňák, Ph.D.
vedoucí katedry

prof. RNDr. Václav Snášel, CSc.
děkan fakulty

Prohlášení studenta

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě, dne: *15. dubna 2016*



……..……
podpis studenta

Poděkování

Rád bych poděkoval mému konzultantovi Ing. Václavu Hrstkovi za umožnění vykonávání odborné individuální praxe v Orchard Hotel a.s. - Park Inn by Radisson Hotel Ostrava, za odbornou pomoc, konzultace a čas věnovaný při vytváření této bakalářské práce.

Dále bych chtěl poděkoval paní Ing. Zdeňce Chmelíkové, Ph.D. za konzultace, semináře a odborný dohled při psaní bakalářské práce.

Prohlášení zástupce spolupracující právnické nebo fyzické osoby

„Souhlasím se zveřejněním této bakalářské práce dle požadavků čl. 26, odst. 9 Studijního a zkušebního řádu pro studium v bakalářských programech VŠB-TU Ostrava."

Dne: *16. dubna 2016*

.....
podpis zástupce

Abstrakt

Bakalářská práce popisuje průběh absolvování odborné praxe ve firmě Orchard Hotel a.s. - Park Inn by Radisson Hotel Ostrava.

V úvodu práce představuji odborné zaměření firmy, mé zařazení v pracovním týmu a popis zadaných úkolů. V dalších částech bakalářské práce jsou podrobně popsány řešení a postupy, které byly zvoleny při praktickém řešení zadaných úkolů, které mají pomoci ke zlepšení, zefektivnění a zabezpečení pracovních podmínek zaměstnanců i hostů.

Závěr práce zahrnuje zhodnocení absolvování odborné praxe a znalostí, které byly získány během studia a pomohly při řešení zadaných úkolů. Rovněž byly analyzovány scházející teoretické a praktické dovednosti v průběhu praxe.

Klíčová slova

Orchard Hotel a.s. - Park Inn by Radisson Hotel Ostrava, odborná praxe, Wi-Fi, AP, HeatMapper, Radius, Cisco, HP, Mikrotik, VPN, OpenVPN, Nagios, NRPE, Linux, Shell, skriptovací jazyky, HTML

Abstract

This bachelor thesis describes the process of passing a practical placement in Orchard Hotel a.s. - Park Inn by Radisson Hotel Ostrava.

In the introduction of this thesis I present the professional focus of the enterprise, my inclusion in the work team and a description of the assigned tasks. Further parts of this thesis include detailed solutions and procedures that have been chosen to solve the tasks, which help to improve, streamline and secure working conditions for employees and guests.

The last part of this work involves a review of the practical placement experience and the knowledge that I gained during studies and that proved to be helpful when solving the tasks. I also analyze missing theoretical and practical skills during my practical placement.

Key words

Orchard Hotel a.s.- Park Inn by Radisson Hotel Ostrava, Professionla practice, Wi-Fi, AP, HeatMapper, Radius, Cisco, HP, Mikrotik, VPN, OpenVPN, Nagios, NRPE, Linux, Shell, scripting languages, HTML

Obsah

Seznam použitých zkratek

Zkratka	Význam
AP	Access Point
CAM	Content Addressable Memory
GB	GigaByte
HP	Hewlett-Packard
HTML	HyperText Markup Language
IP	Internet Protocol
IT	Information Technology
LAN	Local Area Network
LTS	Long Term Support
MAB	MAC Authentication Bypass
MAC	Medium Access Control
NAT	Network Address Translation
OS	Operating Systém
PHP	Hypertext Preprocessor
RADIUS	Remote Authentication Dial In User Service
RAID	Redundant Array of Independent Disks
RB	RouterBoard
RSMA	Reverse polarity SubMiniature version A
SFP	Small Form-factor Pluggable
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSTP	Secure Socket Tunneling Protocol
VLAN	Virtual Local Area Network
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity

Seznam ilustrací a tabulek

Úvod

Úvodem bych Vás chtěl seznámit se svou bakalářskou prací, jejíž náplní bylo absolvování individuální odborné praxe ve firmě Orchard Hotel a.s.- Park Inn by Radisson Hotel Ostrava. Cílem této práce byla deskripce, analýza, a řešení zadaných úkolů.

Práce je rozdělena do pěti hlavních kapitol. V rámci výše uvedené problematiky je první kapitola věnována popisu odborného zaměření firmy a rovněž mého pracovního zařazení v IT oddělení.

Druhá kapitola se zabývá deskripcí hlavních pracovních úkolů a požadavků ze strany společnosti. Zadané pracovní úkoly spočívají v návrhu zabezpečení přístupové vrstvy do firemní sítě na přístupových přepínačích, či zlepšení pokrytí hotelové Wi-Fi sítě pro hosty. Dalším hlavním úkolem je výběr, návrh a konfigurace zařízení pro přístup k internímu webovému serveru. Poslední z úkolů se věnuje rozšiřování monitorovacího systému NAGIOS.

Třetí nosná část obsahuje detailní rozbor postupů řešení výše uvedených jednotlivých úkolů. Na základě analýzy jsou formulovány návrhy řešení, které pomohou hotelu ke zlepšení stávající situace. V neposlední řadě jsou součástí kapitoly také problémy, které se vyskytly v průběhu vypracovávání úkolů. Nakonec je uvedena i podoba finálního nasazeného řešení u každého z úkolů.

V závěru bakalářské práce jsou shrnuty teoretické a praktické znalosti i dovednosti, které jsem získal jak v průběhu vysokoškolského studia, tak během absolvování odborné praxe. Jsou zde také uvedeny znalosti, které mi během praxe scházely. Dále je zhodnocen celkový průběh odborné praxe, dosažené výsledky a jejich časová náročnost.

1 Odborné zaměření firmy Orchard Hotel a.s.

1.1 Odborné zaměření firmy

Orchard Hotel a.s.- Park Inn by Radisson Hotel Ostrava se stal prvním čtyřhvězdičkovým hotelem mezinárodního řetezce v Ostravě a byl postaven v roce 2008. Park Inn je hotelová značka belgické společnosti Rezidor Hotel Group. Hotel je situován v blízkosti centra města, na ulici Hornopolní, vedle kancelářského komplexu Orchard. Disponuje 185 pokoji v designu hotelové značky, moderně zařízeným kongresovým centrem, které nabízí šest jednacích místností. Hlavní kongresový sál pojme až 20 osob. V hotelu nechybí ani wellness a fitness centrum či restaurace Bamboo s celodením provozem. [1]

Hotel obsahuje několik oddělení včetně IT oddělení, které se stará o bezproblémový chod, úpravu a rozvoj záležitostí týkajících se klienských stanic, serverů, podpůrných hotelových systémů, kongresové techniky, telefoních a televizních systémů.

1.2 Popis pracovního zařazení

Ve firmě Orchard Hotel a.s. jsem pod vedením pana Ing. Václava Hrstky vykonával pracovní pozici IT specialisty. Pan Hrstka je také IT manažerem v Park Inn Hotel Prague provozovaný společností Hermitage Holdings s.r.o.. Spolupracoval jsem s panem Hrstkou na chodu ostravského hotelu z podhledu IT oddělení. Náplní práce byla správa firemní hotelové sítě, úprava a rozvoj hotelových a podpůrných systémů. Na tuto pozici jsem nastoupil již v roce 2013 během vysokoškolského studia.

2 Zadané úkoly při vykonávání odborné praxe

2.1 Zabezpečení přístupu do firemní sítě

První ze stěžejních úkolů této odborné praxe spočíval ve zlepšení zabezpečení přístupové vrstvy interní hotelové sítě.

Datové rozvody pro interní síť jsou poměrně rozsáhlé a pokrývají dvě patra budovy. Nacházejí se v nich kanceláře, technické místnosti a další oddělení hotelu, jako např. kuchyň, housekeeping. Část rozvodů zasahuje i do kongresových sálů, které slouží pro připojení interních zařízení do firemní sítě pro schůzky, či porady jednotlivých oddělení.

Úkolem bylo najít vhodné řešení pro zlepšení zabezpečení přístupu do interní hotelové sítě pro jednotlivá síťová zařízení. Nasazené řešení mělo být jednoduché, přehledné a mělo umožnovat jednoduchý dohled a správu nad připojenými a povolenými zařízeními, dále detekci nepovolených zařízení s následnou notifikací prostřednictvím e-mailu.

2.2 Analýza Wi-Fi sítě pro hosty

Druhý ze stěženích úkolů byl zaměřen na zmapování pokrytí Wi-Fi sítě, která je určena pro bezplatný přístup na internet pro hotelové hosty s následnými návrhy na zlepšení. Hlavním důvodem byly časté problémy a stížnosti klientů s připojením, rychlostí a kvalitou signálu bezdrátové sítě. Každé připojené zařízení bylo původně omezeno maximální přenosovou rychlostí 10 Mb/s.

Tento úkol nejprve zahrnoval kontrolu aktuálního počtu a rozmístění jednotlivých přístupových bodů na každem patře budovy podle dodané dokumentace. Následná analýza obsahovala zároveň i měření kvality signálu na jednotlivých pokojích. Pomocí aplikace v mobilním telefonu došlo k vytvoření celkové mapy pokrytí, která simulovala situace hostů, jež se převážně připojují pomocí mobilních telefonů. Získané výsledky byly posléze konzultovány s vedoucím práce a společností Mikenopa a.s., která zajišťuje správu bezdrátové sítě. V praktické části bylo specifikováno několik návrhů na zlepšení kvality signálu včetně jejich následné aplikace do stávající sítě.

Na závěr byla vytvořena webová prezentace sloužící jako podkladová dokumentace při řešení problémů s Wi-Fi sítí. Prezentace obsahuje přehled jednotlivých přístupových bodů (dále AP - Access Point), jejich základní informace, fotografie přesného fyzického umístění po hotelu. Obsahem jsou také výsledky z měření úrovně signálu.

2.3 Návrh firewall/VPN zařízení pro přístup k internímu serveru

Dalším úkolem bylo zjistit aktuální možnosti pro nové zařízení, které mělo sloužit jako firewall a VPN server. Účelem tohoto zařízení bylo umožnit přístup zaměstnanců k webovému serveru jak z interní, tak i z externí sítě. Server hostuje konferenční systém obsahující informace ohledně akcí, profilů pořadatelů a dalších důležitých informací pro obchodní a kongresové oddělení.

Úkolem bylo vybrat vhodné zažízení pro tento účel v rozumném poměru cena a výkon, nastavit pravidla firewallu pro zabezpečení sítě a zvolit vhodný typ VPN serveru pro přístup zaměstnanců

ze zařízení nacházející se mimo interní síť. Finanční limit na toto zařízení byl stanoven v maximální výši 5000 Kč.

2.4 Nagios - monitorování firemní sítě

Poslední ze čtyř hlavních úkolů byl zaměřen na rozšíření monitorovacího systému Nagios. Toto rozšíření spočívalo ve vytvoření skriptů, které jsou využívány pro monitorování zařízení a služeb v interní počítačové síťi. Skritpy zahrnovaly například monitorování jednotlivých disků v diskových polích RAID na serverech, monitorování stavu Radius serveru, kontrolu stavu všech tiskáren a periodické zasílání provozních informací pro dokumentaci. V případě detekce problému s monitorovanými zařízeními nebo službami je IT oddělení notifikováno e-mailem.

2.5 Ostatní práce

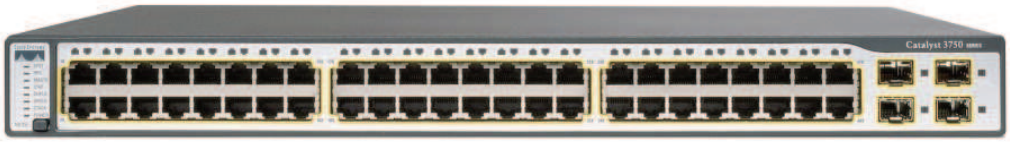
Během odborné praxe jsem se podílel i na dalších úkolech, se kterými se lze běžně potkat na IT oddělení. Tyto práce jsou popsány dále v praktické části.

3 Postup řešení zadaných úkolů

3.1 Zabezpečení přístupu do firemní sítě

Prvním bodem tohoto úkolu bylo zjistit stávají situaci datových rozvodů, použitých druhů a typů síťových zařízení, použitých typů a značek přepínačů v přístupové vrstvě LAN, zjištění možností kontroly přístupu na jednotlivých značkách přepínačů a navrhnout kontrolní server pro správu povolených zařízení.

Zjistil jsem, že datové zásuvky v konferenčních místnostech byly zabezpečeny pomocí plastových zámků, které bylo možné manuálně odstranit, a případné nechtěné zařízení mohlo být připojeno do interní sítě, což byl neakceptující stav. Ostatní datové rozvody byly zakončeny v uzamykatelných kancelářích, ale i přesto mohlo dojít k připojení nevyžádáného zařízení do interní sítě ze strany interních uživatelů a způsobit bezpečnostní problém. Přístupová vrstva lokální sítě se skládá z přepínačů dvou značek. A to ze dvou Cisco přepínačů typu WS-C3750-48PS s čtyřicetiosmi fastethernetovými a čtyřmi Small Form-factor Pluggable (dále SFP) porty. A dále ze dvou přepínačů značky Hewlett-Packard (dále HP), přesněji ProCurve 2824 s dvaceti gigabitovými porty a čtyřmi SFP porty.

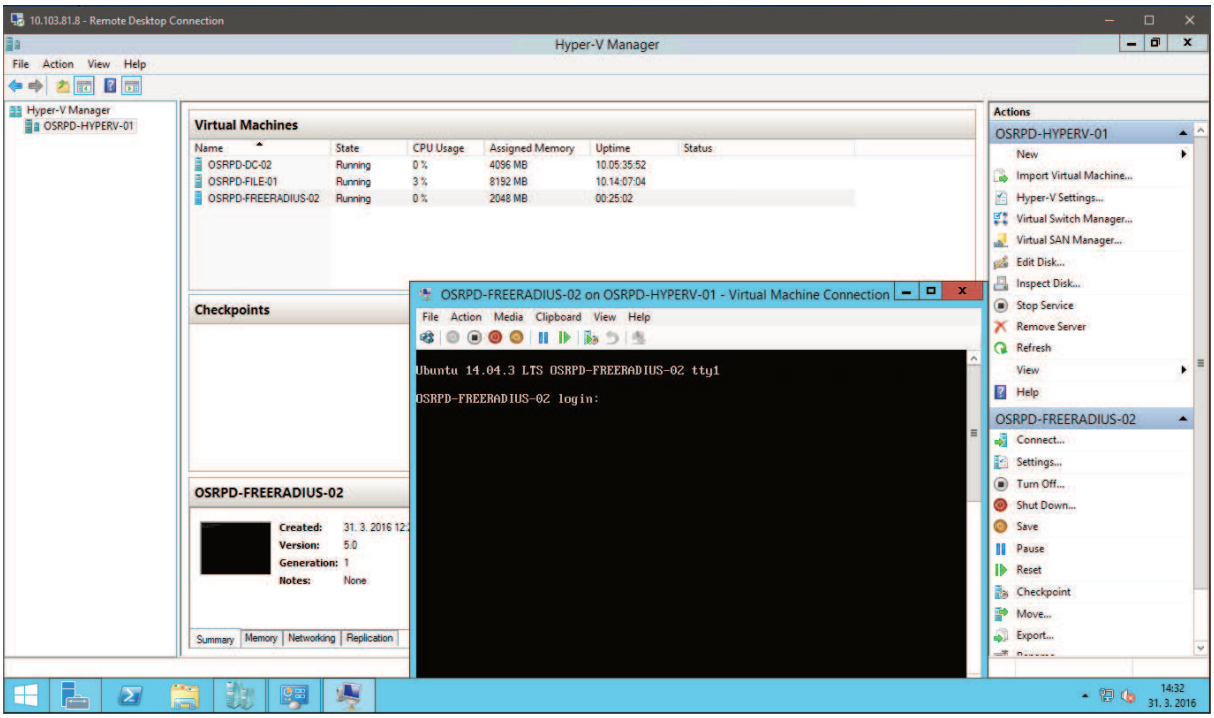


Obrázek 3.1: *Přepínač Cisco Catalyst WS-3750-48P*

Obrázek 3.2: *Přepínač HP ProCurve 2824*

Dalším bodem v řešení tohoto problému bylo zjištění všech typů připojených síťových zařízení. Mezi zařízeními se nacházely klienské stanice, tiskárny, platební a mobilní terminály, IP kamery a VoIP telefony. Celkově bylo identifikováno 80 zařízení, přičemž podstatná většina zařízení nepodporovala žádný bezpečnostní autentizační protokol. Bylo zvoleno jednotné řešení pro všechny zařízení. Autentizace zařízení je vždy prováděna na základě jeho MAC adresy. Tato metoda se také nazývá MAB (MAC-Authentication-Bypass). Jako server je využita volná stanice HP Compaq DC5850. Záložní server je tvořen pomocí virtuálního stroje, který je identický jako hlavní server a beží na Hyper-V serveru.

Obrázek 3.3: *Stanice HP Compaq DC5850 SFF*



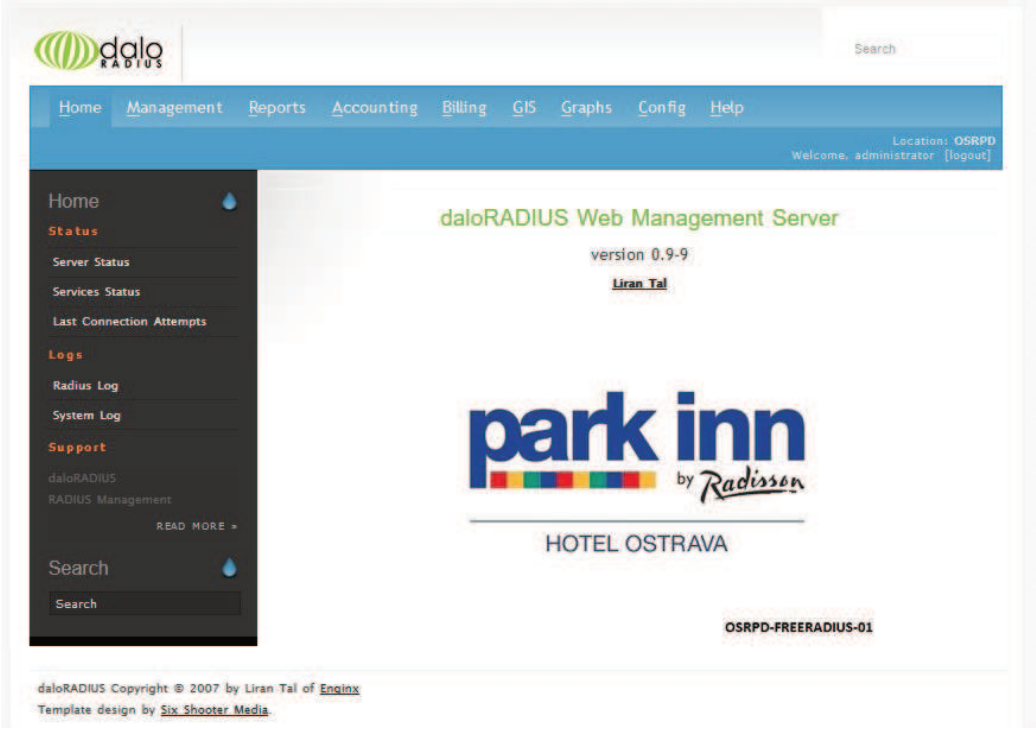
Obrázek 3.*4*: *Záložní virtuální server*

3.1.1 Konfigurace Radius serveru

Tento server je osazen 64-bitovým procesorem Athlon Dual Core, operační pamětí o velikosti 4GB, dále bylo vytvořeno diskové pole RAID, které se skládá ze dvou disků o kapacitě 250 GB. Byl použit RAID typu 1, tzv. zrcadlení, kdy dochází k replikaci obsahů obou disků. Tento typ je nejjednoduší, ochrana dat je efektivní, kdy při výpadku jednoho z disků se pracuje ihned s druhou kopií.

Jako operační systém byl zvolen Linux, přesněji distribuce Ubuntu 14.04 LTS pro servery, dostupná na [2]. Jako Radius server byl použit projekt FreeRadius verze 3, který byl rozšířen o projekt Daloradius 0.9.9, dostupný na [3], který poskytuje nadstavbu pro webovou správu celého Radius serveru. Dále byl doinstalován požadovaný webový server Apache2, databázový server MySQL a PHP verze 5.5. Pro vytvoření a správu RAID pole byla použita utilita mdam. Dále byl mezi hlavním a záložním serverem vytvořen jednoduchý failover cluster pomocí utility ucarp. Při výpadku hlavního serveru se zátěž přesune na záložní server. Každý server má svoji IPv4 adresu a spolu hostují jednu virtuální adresu, se kterou komunitují přepínače.

Po instalaci všech požadovaných balíčků a programů přišla na řadu konfigurace Radius serveru. Byla vytvořena databáze MAC adres všech povolených zařízení, databáze přepínačů a skupiny informací pro výměnu mezi přepínačem a serverem, které obsahují název virtuální sítě LAN (dále VLAN) pro přiřazení portu do správné VLAN. Pro zjišťování MAC adres byly využity CAM tabulky přepínačů, které obsahovaly požadované adresy. Rovněž byla provedena kontrola MAC adres pomocí síťového skeneru Advanced IP Scanner[4].



Obrázek 3.5: *Daloradius*

3.1.2 Konfigurace přepínačů

Na přepináče byly přídány 2 VLANy, jedna slouží pro přístup do interní sítě, druhá je použita pro nepovolené zařízení. Důvod této konfigurace spočíval v zamezení odposlechu všesměrového vysílání a tím také případnému odposlechu akceptovatelné MAC adresy.

```
OSRPD-SW4#sho vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa1/0/1, Fa1/0/2, Fa1/0/3
                                                Fa1/0/4, Fa1/0/5, Fa1/0/6
                                                Fa1/0/7, Fa1/0/11, Fa1/0/14
                                                Fa1/0/15, Fa1/0/16, Fa1/0/17
                                                Fa1/0/18, Fa1/0/19, Fa1/0/20
                                                Fa1/0/21, Fa1/0/22, Fa1/0/23
                                                Fa1/0/24, Fa1/0/25, Fa1/0/26
                                                Fa1/0/27, Fa1/0/28, Fa1/0/29
                                                Fa1/0/30, Fa1/0/31, Fa1/0/32
                                                Fa1/0/33, Fa1/0/34, Fa1/0/35
                                                Fa1/0/36, Fa1/0/37, Fa1/0/38
                                                Fa1/0/39, Fa1/0/40, Fa1/0/41
                                                Fa1/0/42, Fa1/0/43, Fa1/0/44
                                                Fa1/0/45, Fa1/0/46
81   OSRPD                            active    Fa1/0/8, Fa1/0/9, Fa1/0/10
                                                Fa1/0/12, Fa1/0/13, Fa1/0/47
                                                Fa1/0/48, Gi1/0/1, Gi1/0/2
                                                Gi1/0/3, Gi1/0/4
```

Obrázek *3.6: Nastavené VLANy na přepínačích*

Dále byl celý přepínač nastaven tak, aby využíval Radius server pro autentizaci zařízení. Byl přídán záznam pro IPv4 adresu RADIUS server s definicí portů pro ověření a účtování. Pro autentizaci byl použit standardní port 1812, pro účtování 1813. Bylo nastaveno také bezpečnostní heslo pro ověření přepínače vůči serveru.

```
OSRPD-SW4#show radius server-group all
Sever group radius
    Sharecount = 1  sg_unconfigured = FALSE
    Type = standard  Memlocks = 1
    Server(10.103.81.99:1812,1813) Transactions:
    Authen: 352 Author: 0       Acct: 453
```

Obrázek 3.7: *Nastavený záznam pro Radius server*

Jednotlivé přístupové porty byly nastaveny tak, aby vyžadovaly autentizaci připojených zařízení pomocí metody MAB.

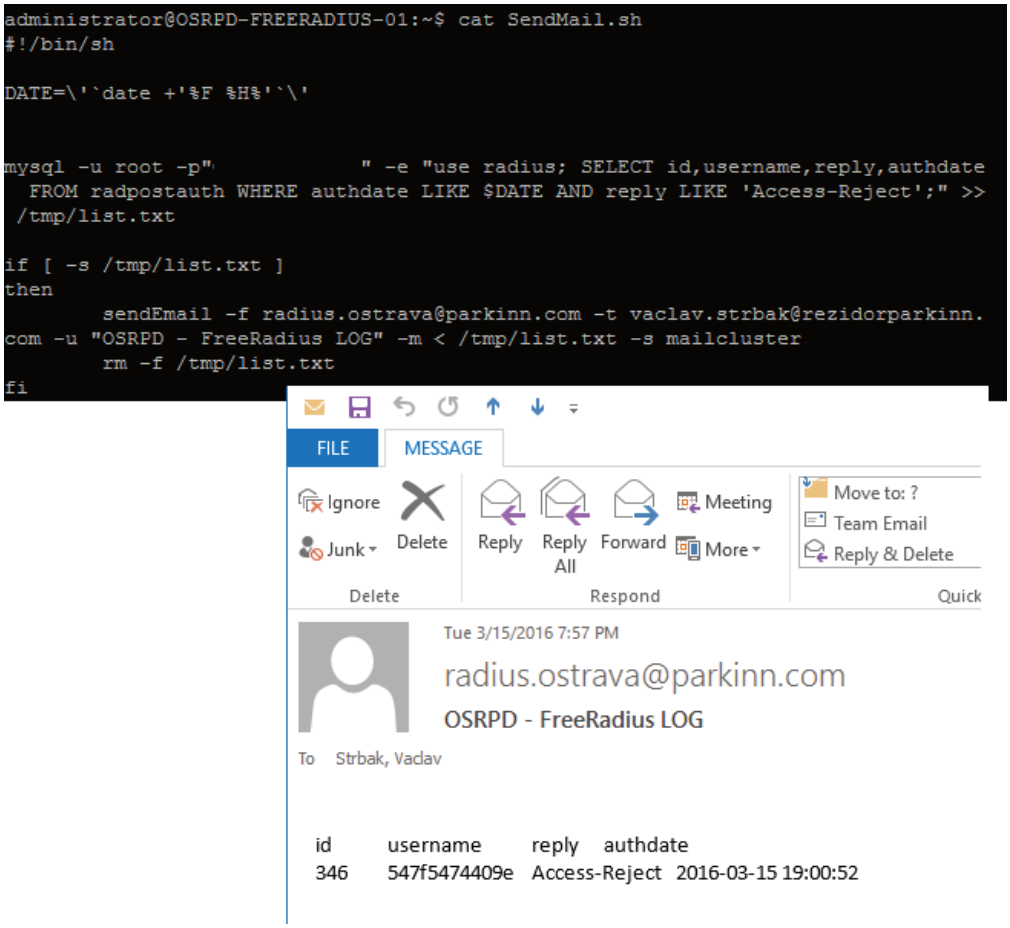
```
interface FastEthernet1/0/1
 switchport mode access
 authentication host-mode multi-auth
 authentication port-control auto
 authentication timer restart 900
 mab
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet1/0/2
 switchport mode access
 authentication host-mode multi-auth
 authentication port-control auto
 authentication timer restart 900
 mab
 spanning-tree portfast
 spanning-tree bpduguard enable
```

Obrázek 3.8: *Nastavení portů na Cisco přepínačích*

Posledním krokem v konfiguraci bylo nastavení administrátorského učtu, hesla a SSH přístupu pro vzdálenou konfiguraci přepínače.

3.1.3 Notifikace nepovoleného zařízení

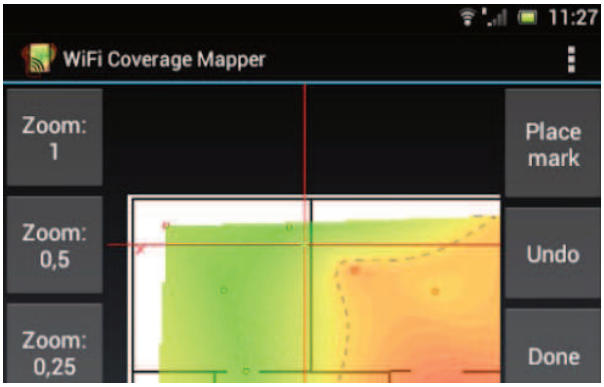
Pro případy, kdy se do interní hotelové sítě chce připojit nepovolené zařízení, je toho zařízení blokováno a IT oddělení upozorněno e-mailem. Pro notifikaci byl na Radius serveru vytvořen cron obsahující skript, který z databáze s pokusy o připojení vyfiltruje záznamy odmítnutých autentizací a poté pošle e-mail členům IT oddělení.



Obrázek 3.9: *Ukázka notifikace při odmínutí přístupu*

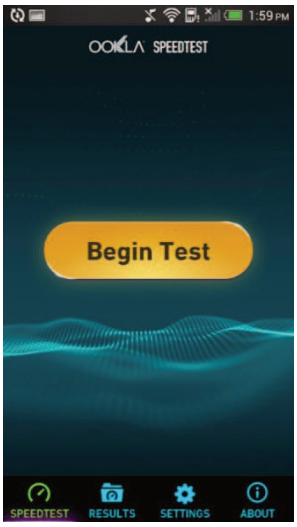
3.2 Analýza Wi-Fi sítě pro hosty

Při řesení tohoto úkolu byla situace podobná. Jako první byla provedena kompletní kontrola, jak po stránce fyzického rozmístění přístupových bodů a rozvodů, tak také z hlediska úrovně signálu v rámci celého hotelu. Pro zjištování kvality signálu byly využity mobilní aplikace Wi-Fi Coverage Mapper, WiFi Analyzer a SpeedTest pro systém Android, které lze stáhnout na [5], [6], [7]. Pomocí aplikace Wi-Fi Coverage Mapper lze vytvářet teplotní mapy signálu. Nevýhodou je však nemožnost ukládát rozpracované mapy, což zapříčinilo, že měření muselo být provedeno najednou. Aplikace umožňuje nahrát obrázek poschodí, který slouží jako podklad pro vytvoření teplotní mapy. WiFi Analyzer a Speedtest byly použity pro detailní zjištění úrovně signálu a přenosové rychlosti na jednotlivých pokojích.



Obrázek 3.10: *Aplikace WiFi Coverage Mapper*

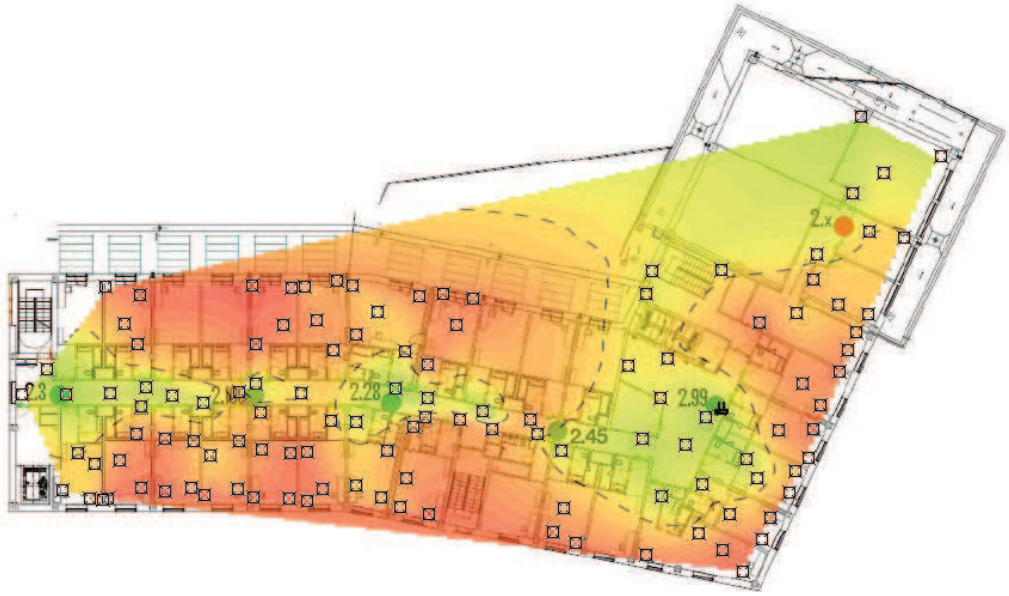
Obrázek 3.11: *Aplikace WiFi Analyzer*



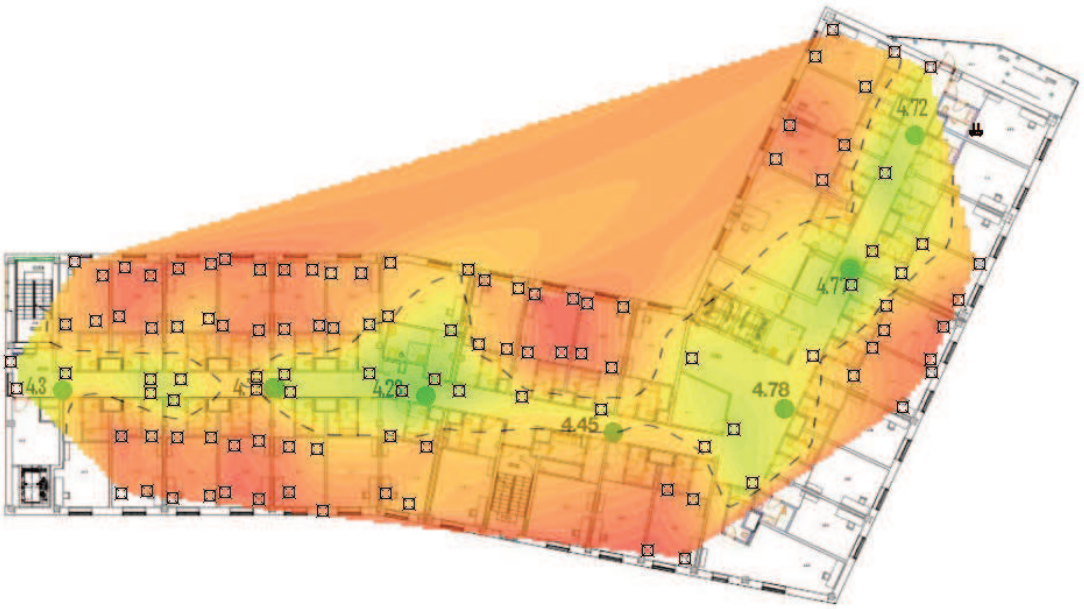
Obrázek 3.12: *Aplikace SpeedTest*

Po provední prvotní kontroly přístupových bodů bylo oproti dodané dokumentaci zjišteno, že některé AP nebyly vůbec nasazeny, případně byly umístěny v nevhodných místech nebo byly antény natočeny nesprávným směrem. Naměřené přenosové rychlosti se neshodovaly s požadovanými. Použitým typem již nasazených přístupových bodů byl Cisco AIR-LAP1242AG-A-K9.

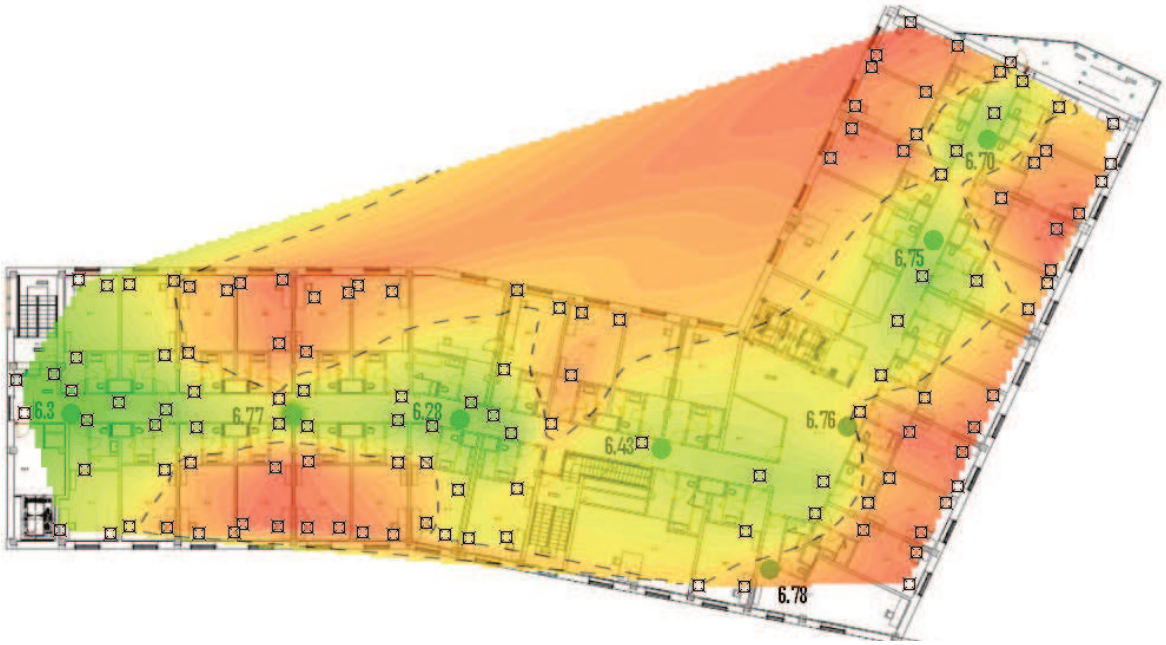
Na následujících obrázcích můžeme vidět výsledky první kontroly kvality signálu na vybraných patrech.



Obrázek 3.13: *První kontrolní měření - 1. patro*



Obrázek 3.14: *První kontrolní měření - 3. patro*



Obrázek 3.15: *První kontrolní měření - 5. patro*

Tabulka 3.1. *Naměřené hodnoty některých pokojů v levém traktu 5. patra po první kontrole*

	Přen. rychlost Dow / Up [Mb/s]		Úroveň signálu [dBm]	
Místo měření	Stůl	Pohovka	Stůl	Pohovka
Pokoj 533	6 / 10	10 / 10	-78	-75
Pokoj 534	8 / 10	10 / 4	-80	-82
Pokoj 535	6 / 3	3 / 4	-85	-85
Pokoj 536	4 / 4	2 / 2	-87	-86
Pokoj 537	6 / 4	5 / 4	-85	-84
Pokoj 538	2 / 3	3 / 1	-89	-86
Pokoj 539	2 / 1	5 / 2	-86	-84

Součástí tohoto úkolu bylo vytvoření jednoduché webové prezentace. Využil jsem technologie HTML a Javascript. Prezentace slouží jako pomocník při řešení incidentů s připojením nebo nízkou úrovní signálu.

Room:	Home	FLOOR_1	FLOOR_2	FLOOR_3	FLOOR_4	FLOOR_5	FLOOR_6	FLOOR_0	FLOOR_BASEMENT
Map - Signal	Home	FLOOR_1	FLOOR_2	FLOOR_3	FLOOR_4	FLOOR_5	FLOOR_6	FLOOR_0	FLOOR_BASEMENT

Floor 1

Maps

Oznaceni AP	MAC adresa	Stav	Cislo zasuvky	Mikenopa switch/port
AP-1.1	00-1E-BE-27-22-52	OK	2.3	CZOSPIN-G-SW-1-12 / 14
AP-1.2	00-1F-CA-27-91-E2	OK	2.100	CZOSPIN-G-SW-1-12 / 15
AP-1.3	00-1E-BE-27-1F-50	OK	2.28	CZOSPIN-G-SW-1-12 / 16
AP-1.4	00-1F-CA-27-F0-7C	OK	2.45	CZOSPIN-G-SW-1-12 / 17
AP-1.5	00-1E-BE-27-20-8C	OK	2.99	CZOSPIN-G-SW-1-12 / 2
AP-1.6	7C-0E-CE-85-78-17	OK	2.58	CZOSPIN-G-SW-1-12 / 10

Obrázek 3.16: *Ukázka webové prezentace Wi-Fi sítě*

Díky těmto naměřeným výsledkům a dokumentaci jsme zahájili konzultace s firmou Mikenopa a.s., která v hotelu Park Inn Ostrava zajišťuje správu bezdrátové sítě pro hosty. Z jejich strany byla provedena kontrola konfigurace sítě. Bylo zjištěno, že vysílácí výkon všech přístupových bodů nebyl nastaven na maximální výkon. Došlo tedy k úpravě konfigurace a také byla na jejich doporučení zakoupena uvedená zařízení, 4x Cisco AIR-CAP1702I-E-K9, 5x Cisco AIR-SAP1602I-N-K9 a 1x Mikrotik RB951-2nD pro posílení dosahu signálu.

Obrázek 3.17: *Cisco AIR-SAP1605I-N-K9*

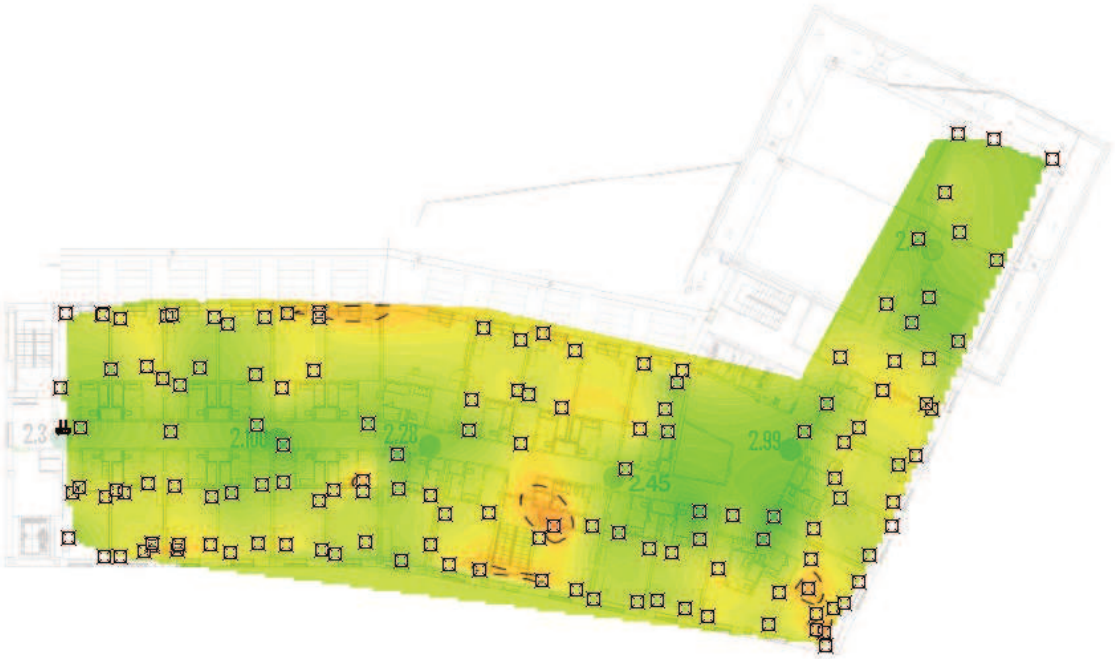
Obrázek 3.18: *Cisco AIR-CAP1702I-E-K9*

Druhý krok zahrnoval nasazení zakoupených AP a úpravu stávajících tak, aby signál na pokojích byl dostačující. V některých případech, kdy úroveň signálu nebyla v pokojích akceptována, jsme po konzultaci s panem Hrstkou dodatečně zakoupili čtyři externí stropní 2,4 GHz antény, které jsme umístili na podhledy v chodbách. Zvoleným typem byly všesměrové antény 2,4 GHz Alfa ACA-001, se ziskem 5 dBi a koncovkou RSMA male.

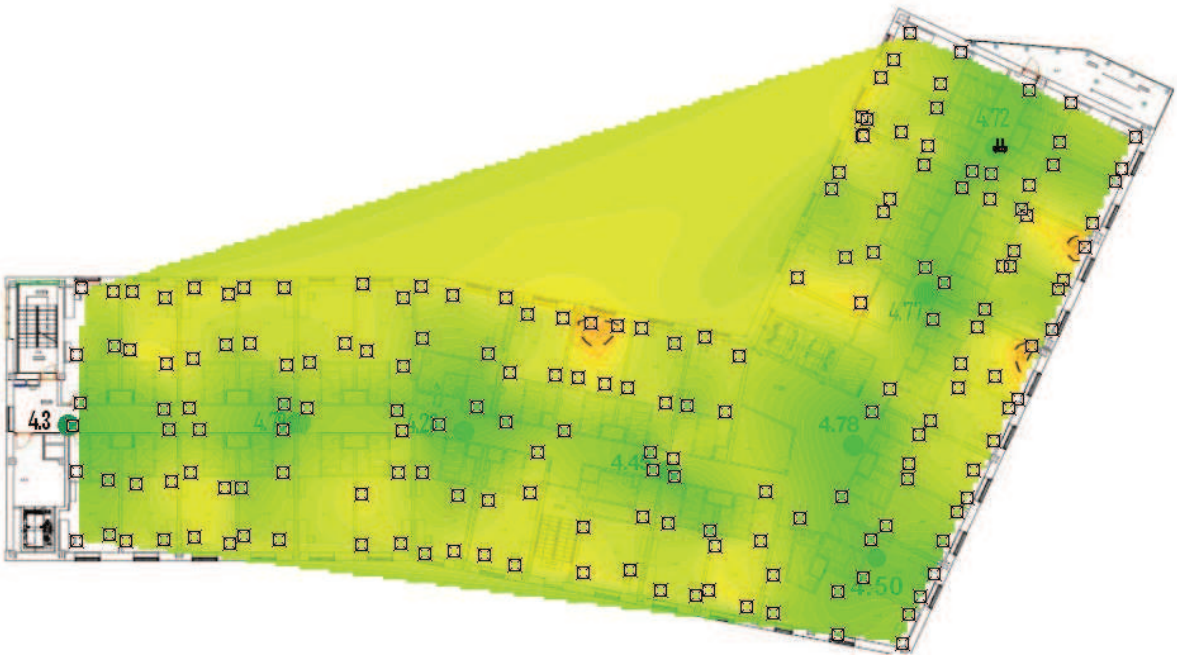
Obrázek 3.19: *Všesměrová externí anténa Alfa ACA*-001

V poslední části byla provedena finální kontrola veškerých přístupových bodů a kvality signálu ve všech patrech hotelu. V závěrečném měření byla maximální přesnosová rychlost pro připojená zařízení navýšena na 30Mb/s. Minimální akceptovatelná přenosová rychlost byla stanovena na 8 Mb/s, která byla po závěrečné kontrole dodržena na všech pokojích.

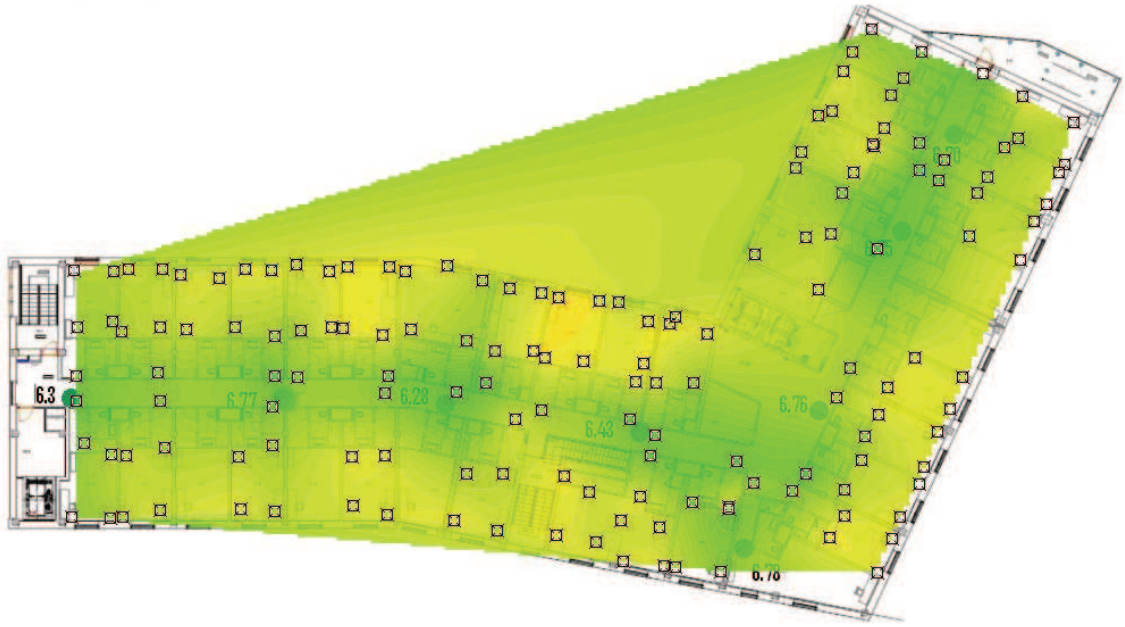
Na následujících obrázcích můžeme vidět výsledky poslední kontroly úrovně signálu provedných na stejných patrech jako v prvním měření.



Obrázek 3.20: *Poslední kontrola měření - 1. patro*



Obrázek 3.21: *Poslední kontrolní měření - 3. patro*



Obrázek 3.22: *Poslední kontrola měření - 5. patro*

Tabulka 3.2. *Naměřené hodnoty pokojů v levém traktu 5. patra po poslední kontrole*

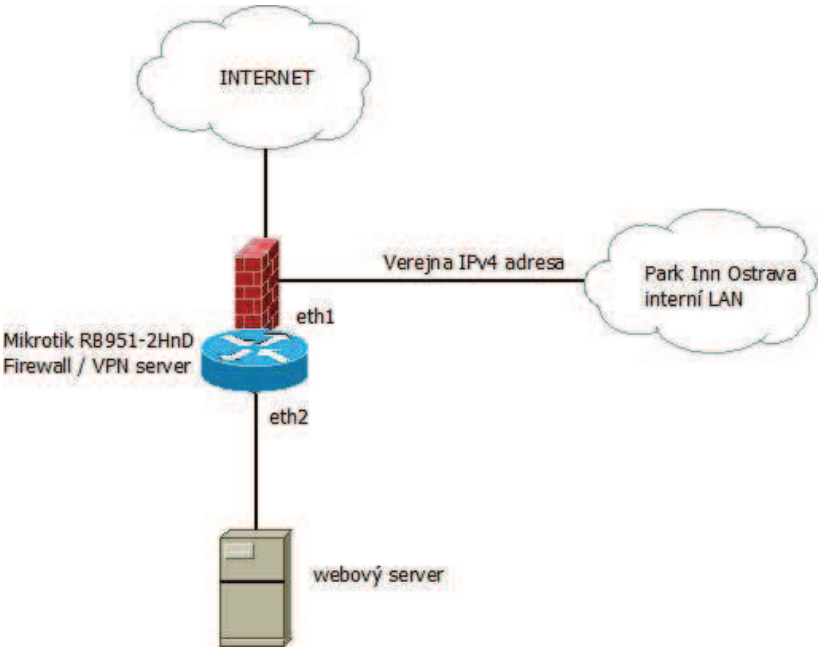
	Přen. rychlost Down / Up [Mb/s]		Úroveň signálu [dBm]	
Místo měření	Stůl	Pohovka	Stůl	Pohovka
Pokoj 533	16 / 14	17 / 15	-64	-65
Pokoj 534	13 / 14	13 / 13	-65	-63
Pokoj 535	13 / 13	14 / 16	-65	-64
Pokoj 536	14 / 16	14 / 15	-66	-67
Pokoj 537	18 / 17	18 / 17	-64	-64
Pokoj 538	14 / 15	15 / 15	-65	-67
Pokoj 539	14 / 15	18 / 16	-68	-64

3.3 Návrh firewallu/VPN pro přístup k webovému serveru

Při výběru zařízení jsme se rozhodovali mezi dvěma zařízeními značky Mikrotik, a to mezi RB951-2HnD s pěti gigabitovými porty a RB/2011L-IN se čtyřmi gigabitovými a fastethernetovými porty. Nakonec byl zvolen prvně jmenovaný. Důvodem byla menší velikost zařízení, identická výkonnost, nadbytečné fastethernetové porty u druhého typu a dobrý poměr cena/výkon. Výběr značky Mikrotik byl dán i mou osobní znalostí a zkušeností konfigurace systému MikrotikOS.

Obrázek 3.23: *Mikrotik RB951-2HnD*

Na níže uvedeném obrázku můžeme vidět zjednodušené schéma zapojení Mikrotiku a webového serveru.



Obrázek 3.24: *Zjednodušené schéma zapojení firewall/VPN zařízení*

Konfiguraci směrovače jsem si kontroloval pomocí dokumentace pro MikrotikOS, dostupné na [8]. Přístup na webový server z interní sítě jsem vyřešil použitím NAT (Network Address Translation), přesněji nastavením pravidel pro přesměrování portů z veřejné IPv4 adresy směrovače

na privátní IPv4 adresu webového serveru pro porty 80 a 443. Stejný postup jsem použil i pro port 22, který využívá Winbox ke konfiguraci samotného směrovače.

Pro vzdálený přístup jsem se rozhodoval mezi protokoly SSTP, L2TP s IPsec a projektem OpenVPN.

SSTP (Secure Socket Tunneling Protocol) je protokol pro tunelová propojení, který pomocí protokolu HTTPS na portu Tcp 443 přenáší data přes brány firewall a webové proxy servery, které by mohly blokovat přenosy pomocí protokolů PPTP a L2TP/IPsec. Protokol SSTP poskytuje mechanismus pro zapouzdření přenosu protokolu PPP prostřednictvím kanálu SSL (Secure Sockets Layer) protokolu HTTPS. Využití protokolu PPP přináší podporu silných metod ověřování jako je protokol EAP-TLS. Protokol SSL poskytuje zabezpečení na úrovni přenosu a přináší vylepšené vyjednávání klíčů, šifrování a kontrolování integrity.[9] Jelikož zaměstnanci používají různé značky zařízení s různými operačními systémy musel jsem upustit od tohoto protokolu. SSTP nativně podporuje pouze operační systémy Microsoftu. Pro operační systém Android nebo iOS by se musela doinstalovat placená aplikace.

Protokol L2TP (Layer Two Tunneling Protocol) je také tunelovací protokol pro podporu virtuálních privátní sítí (dále VPN - Virtual Private Network), který je rozšířen pomocí IPSec (Internet Protocol security). Kombinace protokolu L2TP a IPSec se označuje jako připojení L2TP/IPSec. L2TP/IPSec zabezpečuje základní služby virtuální privátní sítě, tedy zapouzdření a šifrování soukromých dat.[9] Nevýhodou tohoto řešení je nutnost povolení portů číslo 50,1701 a 4500, které většina internetových poskytovatelů blokuje a mohl by nastat problém při připojování zaměstnanců.

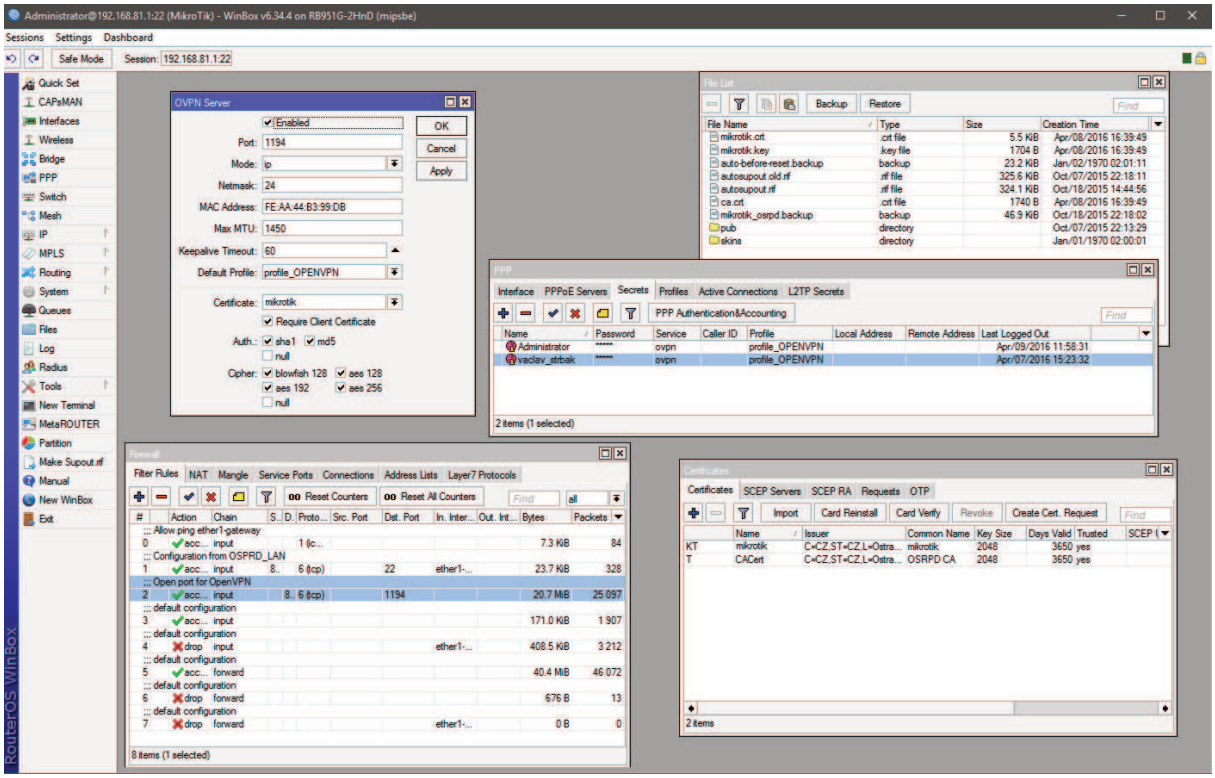
Jako vhodné řešení byl nakonec použit projekt OpenVPN. Je to volně dostupný software, který dokáže vytvořit šifrovaný VPN tunel mezi hostitelskými stanicemi. S využitím architektury klient-server je schopný zajistit přímé spojení mezi počítači za NATem bez jakékoliv potřeby NAT konfigurovat. [10]

Prvotním krokem bylo vytvoření certifikační autority, jednotlivých certifikátů pro VPN server a uživatele pomocí nástroje Easy RSA. Při vytváření certifikátů bylo nutno nejprve vyplnit konfigurační soubor easy-rsa/vars potřebnými informacemi. Následně pomocí příkazu ./build-ca došlo k vytvoření certifikační autority včetně souborů ca.crt a ca.key. Pomocí příkazů./build-key a ./build-key-server jsem vytvořil certifikáty pro uživatel a VPN server.

```
root@UBUNTU-SERVER01:/etc/openvpn/easy-rsa# ./build-ca
root@UBUNTU-SERVER01:/etc/openvpn/easy-rsa# ./build-key-server mikrotik
root@UBUNTU-SERVER01:/etc/openvpn/easy-rsa# ./build-key vaclav strbak
root@UBUNTU-SERVER01:/etc/openvpn/easy-rsa/keys_old# ls
ca.crt  ca.key  mikrotik.crt  mikrotik.csr  mikrotik.key  serial  serial.old
vaclav_strbak.crt  vaclav_strbak.csr  vaclav_strbak.key  vaclav.txt
```

Obrázek 3.25: *Tvorba certifikátů pomocí Easy RSA*

Následovalo nahrání vytvořených certifikátů na Mikrotik pomocí WinBoxu a nastavení OpenVPN serveru a vytvoření jednotlivých profilů pro každého uživatele na Mikrotiku.



Obrázek 3.26: *Nastavení OpenVPN na Mikrotiku*

Pro každého uživatele jsem vytvořil jeho vlastní .ovpn profil, který slouží při importu VPN připojení na jednotlivých zařízeních. Profil obsahuje nutné informace při sestavování zabezpečeného spojení, certifikát certifikační autority, klientský certifikát a klíč.

```
client
proto tcp
remote  <mikrotik ip>   1194
dev tun
resolv-retry infinite
nobind
persist-key
persist-tun
float
mssfix 1459
tun-mtu 1400
redirect-gateway def1 bypass-dhcp
dhcp-option DNS 192.168.81.1
dhcp-option DOMAIN conference.local
register-dns
cipher AES-256-CBC
auth SHA1

auth-user-pass

<ca>
</ca>

<cert>
</cert>

<key>
</key>
```

Obrázek 3.27: *Uživatelský profil .ovpn*

Po prvotní konfiguraci jsem provedl ověření a otestování pravidel firewallu a nastavení VPN serveru pro vzdálený přístup. Po úspěšném testování a uložení konfigurace jsem provedl kompletní

zálohu nastavení celého Mikrotiku. Dalším krokem bylo přenesení webového serveru, o které se postaral pan Hrstka. Poté následovalo spuštění reálného provozu. Nakonec jsem provedl základní seznámení uživatelů s přístupem na webový server a vytvoření interního návodu pro vytváření VPN připojení na různých zařízeních se systémy Android, iOS či Windows.

3.4 Nagios - monitorování firemní sítě

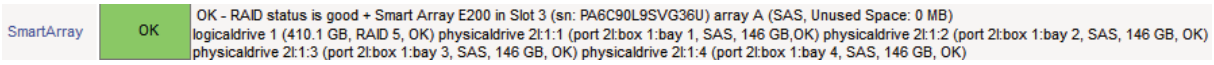
Již při mém nástupu byl nasazen monitorovací systém Nagios. Je to populární open source systém pro automatizované sledování stavu počítačových sítí a jimi poskytovaných služeb. Je vydáván pod licencí General Publix License (dále GPL), vyvíjen a udržován Ethanem Galstadtem a dalšími vývojáři pluginů.[11]

Pro sbírání informací využívá Nagios protokol Simple Network Management Protokol (dále SNMP). Jedná se o standardizovaný protokol aplikační vrstvy, který se používá k monitorování a správě sítě a síťových zařízení. Byl vyvinut s ohledem na rozvoj a rozšiřování počítačových sítí tak, aby umožňoval vzdálenou správu síťových prvků a podrobnější nepřetržitý dohled. V roce 1989 vyšla první verze protokolu SNMPv1.

Do druhé verze protokolu SNMP s označením SNMPv2 nebo SNMPv2c, byla přidána kontrola doručení zprávy. Třetí verze SNMPv3 nabízí navíc i šifrování komunikace, včetně ověření uživatele.[12]

Mým úkolem bylo rozšířit tento systém, který zpočátku monitoroval základní informace na třech serverech jako vytížení procesoru, využití operační paměti, počet bežících procesů a kapacitu disků.

Servery jsou značky HP ProLiant DL385 G2 s operačním systémem Windows. Na serverech jsou nastavena disková pole RAID typu 1+0. Stav disků bylo možné kontrolovat pouze ručně, a to pomocí aplikace HP System Management Homepage, což bylo neefektivní. Bylo potřeba vytvořit skript pro případ, kdyby některý z disků odešel. Jelikož nešlo přímo získávat informace z HP System Management Homepage pro Nagios, na servery jsem nainstaloval Nagios Remote Plugin Executor (dále NRPE) agenty, kteří na vyžádání provedou powershellový skript a vrátí informace o diskovém poli zpátky Nagiosu, jenž vyhodnotí situaci. Při vytváření skriptu jsem využil stránky s pluginy pro Nagios. Podobný skript, který jsem z větší části použil a upravil pro potřeby IT oddělení, můžeme nalézt na [13].



Obrázek 3.28: *Nagios - kontrola pole RAID*

Dalším zahrnutým zařízením pro monitorování byl výše uvedený server Radius. Běžné monitorovací informace jako stav CPU, RAM, byly rozšířeny o informace ohledně stavu pole RAID, stavu daemona ucarp pro failover cluster.

OSRPD-FREERADIUS-01	Current Load	OK	03-31-2016 14:26:30	40d 19h 2m 46s	1/3	OK - load average: 0.00, 0.00, 0.00
	Current Users	OK	03-31-2016 14:19:56	40d 18h 59m 20s	1/3	USERS OK - 1 users currently logged in
	HTTP	OK	03-31-2016 14:23:23	40d 18h 55m 53s	1/3	HTTP OK: HTTP/1.1 302 Found - 406 bytes in 0.034 second response time
	RAID	OK	03-31-2016 14:27:08	9d 22h 12m 8s	1/3	OK - Checked 2 arrays. md1 : active raid1 sda2[0] sdb2[1] md0 : active raid1 sdb1[1] sda1[0]
	Root Partition	OK	03-31-2016 14:23:14	40d 19h 6m 2s	1/3	DISK OK - free space: / 49489 MB (94% inode=96%):
	SSH	OK	03-31-2016 14:26:40	9d 22h 12m 36s	1/3	SSH OK - OpenSSH_6.6.1p1 Ubuntu-2ubuntu2 (protocol 2.0)
	Swap Usage	OK	03-31-2016 14:20:06	40d 18h 59m 10s	1/3	SWAP OK - 95% free (7018 MB out of 7438 MB)
	Total Processes	OK	03-31-2016 14:23:32	40d 18h 55m 44s	1/3	PROCS OK: 159 processes with STATE = RSZDT
	UCARP	OK	03-31-2016 14:25:24	9d 22h 19m 1s	1/3	eth0:ucarp OSRPD-FREERADIUS-01

Obrázek 3.29: *Nagios - kontrola Radius serveru*

V posledním kroku byly nasazeny skripty pro monitorování všech tiskáren pomocí SNMP protokolu. Potřebnými monitorovacími informacemi byly úrovně toneru a počty vytištěných stránek. Tyto informace slouží pro přehled využívání tiskáren a k zápisu do dokumentace. Pro zápis do dokumentace jsem ještě vytvořil skript napsaný v bashi. Požadované informace o tiskárnách jsou poslány jako textová příloha e-mailové zprávy. Tuto přílohu následně zpracuji pomocí dalšího powersheel skriptu, který provede zápis informací do excelové tabulky. Díky tomuto řešení není nutné požadované informace vypisovat ručně. Celkový proces je zminimalizován na stažení textového souboru a spuštění skriptu pro zápis do dokumentace.

3.5 Ostatní práce

Během absolvování odborné praxe, ale i mimo ni, jsem pracoval na běžných činnostech IT oddělení. Mezi tyto činnosti patří například instalace a upgrade nových a stávajících počítačů, IT školení nových zaměstnanců hotelu, podpora uživatelů při řešení hardwarových nebo softwarových problémů. Náplň práce zahrnovala mimo jiné také aktualizaci dokumentace počítačové sítě. Jako technická podpora jsem se dále účastnil akcí pořádané hotelem.

4 Teoretické a praktické znalosti a dovednosti

4.1 Uplatnění znalostí a dovedností získané studiem

Při absolvování odborné praxe jsem se mohl opřít o znalosti a dovednosti, které jsem nabyl studiem vybraných předmětů na Vysoké škole báňské - Technické univerzitě Ostrava.

Mezi nejdůležitější předměty, které mi přinesly potřebné vědomosti při realizaci zadaných úkolů odborné praxe, patřily Počítačové sítě, Telekomunikační sítě a Praktikum komunikačních sítí I. Vědomosti z těchto předmětů mi byly nápomocny při řešení úkolů ohledně zabezpečení přístupové vrstvy interní počítačové sítě, konfigurace nastavení přepínačů a Radius serveru.

Při řešení problému s pokrytím hotelu bezdrátovou sítí mi pomohly především vědomosti a praktické znalosti z předmětu Radiokomunikační technika I. Díky tomuto předmětu jsem dokázal porozumět šíření radiofrekvenčního signálu, orientovat se v různých typech antén a jejich vlastnostech a použitých konektorech při instalaci externích antén.

Znalosti získané z předmětu Přenos dat jsem využil při rozhodování, výběru typu šifrování a zabezpečení VPN severu a jeho konfigurace.

Také i volitelný předmět Správa Windows Systémů mi byl nápomocen při řešení problému na klientských stanicích i serverech s operačními systémy firmy Microsoft.

4.2 Scházející teoretické a praktické znalosti

Během absolvování odborné praxe mi scházely podrobnější znalosti ohledně celkového postupu při řešení větších problémů ve firmě. Například plánování nárhu řešení, vytvoření časového harmonogramu a následná realizace, nebo také vzájemná kooperace s externími firmami zajišťující podporu pro jednotlivé hotelové systémy.

Musel jsem si také osvojit detailnější znalost systému Ubuntu a jeho konfigurace jako Radius serveru. Limitovala mne také neznalost příkazů pro konfiguraci HP přepínačů. Nicméně jsem následně zjistil, že příkazy jsou obdobné jako u společnosti Cisco.

Dále jsme měl také nedostatky ohledně monitorovácího systému Nagios a protokolu SNMP, případně MySQL databáze, kdy jsem nastudoval a používal dokumentaci nebo odborná fóra na internetu zabývající se touto tématikou.

5 Dosažené výsledky a celkové hodnocení odborné praxe

5.1 Dosažené výsledky

Všechny výše uvedené úkoly byly realizovány, úspešně dokončeny a nasazeny. Prostřednictvím prvního úkolu došlo ke zvýšení zabezpečení lokální počítačové sítě před vstupem nežádoucích zařízení. Díky nasazené nadstavbě Daloradius může IT oddělení lépe spravovat povolené zařízení a monitorovat aktivní připojené zařízení. Realizací druhého úkolu byla zlepšena kvalita Wi-Fi sítě pro bezplatný přístup hostů na internet, kdy se při posledním měření nejhorší dosažená rychlost pohybovala okolo 8 Mb/s. Navýšením rychlosti došlo ke zvýšení spokojenosti hostů s nabízenými službami hotelu. Nastavením Mikrotiku jako firewallu a VPN serveru může obchodní oddělení či kompetentní zaměstnanci lépe přistupovat ke konferenčnímu systému, na kterém jsou uložené veškeré důležité informace. Díky VPN přístupu mohou zaměstnanci pracovat i na mobilních zařízeních mimo hotelovou síť. V posledním hlavním úkolu byly pomocí protokolu SNMP nebo pluginu NRPE monitorovány důležité prvky počítačové sítě.

Aktivně jsem se podílel a byl nápomocen během řešení ostatních úkolů (např. upgrade klientských stanic, problémy s hardwarem či softwarem, vytváření dokumentace počítačové sítě, školení nových uživatelů).

5.2 Časová náročnost úkolů

Tabulka 5.1. *Časová náročnost úkolů*

Zadaný úkol	**Počet dnů**
Zabezpečení přístupové vrstvy	10
Zlepšení Wi-Fi sítě	15
Mikrotik - VPN/firewall	4
Nagios - monitorovací systém	2
Upgrade klientských stanic	5
IT školení zaměstnanců	3
Dokumentace	2
Technická podpora	4
Ostatní úkoly	7

Závěr

Absolvování odborné praxe ve firmě Orchard Hotel a.s. Park Inn by Radisson mi přineslo velmi mnoho praktických zkušeností, detailnějších vědomostí při řešení jednotlivých úkolů a také začlenění do pracovního procesu a kolektivu firmy. Doufám, že nabyté informace dále využiji ve své pracovní kariéře.

Prohloubil jsem si znalosti ohledně počítačových sítí, konfigurace jednotlivých zařízení jako jsou například přepínače, směrovače, firewally či VPN servery. Přínosem byla rovněž tvorba dokumentace a návodů pro případnou úpravu konfigurace jednotlivých zařízení. Získal jsem detailnější znalosti o operačním systému Linux a konfigurace jeho možných služeb v rámci počítačové sítě. Osvojil jsem si nejen postupy při řešení jednotlivých úkolů, ale také možnosti vzájemné spolupráce s externími firmami.

Na druhou stranu si myslím, že absolvování odborné praxe bylo přínosem i pro firmu Orchard Hotel a.s.. Realizace zadaných úkolů pomohla ke zvýšení zabezpečení lokální počítačové sítě před přístupem nežádoucích zařízení a případným bezpečnostním incidentem. Dále ke zlepšení kvality poskytovaného bezdrátového připojení na internet, a tím i zlepšení spokojenosti hostů s nabízenými službami. V neposlední řadě došle k zefektivnění práce obchodního oddělení díky přístupu na webový server s konferenčním systémem z externí sítě. Rozšířením monitorovacího systému Nagios má IT oddělení také lepší přehled a kontrolu nad jednotlivými zařízeními v počítačové síti.

Odbornou praxi hodnotím velmi pozitivně a vřele doporučuji jako formu vykonání bakalářské práce. Myslím si, že jakákoliv praxe v oboru je přínosem pro každého studenta, který si začíná budovat svou pracovní kariéru.

Použitá literatura

[1] Hotel Ostrava - Park Inn by Radisson. Park Inn by Radisson Hotels [online]. Ostrava: The Carlson Rezidor Hotel Group., 2016 [cit. 2016-04-01]. Dostupné z: http://www.parkinn.cz/hotel-ostrava.

[2] Ubuntu 14.04 LTS [online]. [cit. 2016-04-01]. Dostupné z: http://www.ubuntu.cz/ziskejte/stahnout

[3] Daloradius 0.9-9 [online]. [cit. 2016-04-01]. Dostupné z: https://sourceforge.net/projects/daloradius/

[4] Advanced IP Scanner. [online]. [cit. 2016-04-01]. Dostupné z: http://www.advanced-ip-scanner.com

[5] Wi-Fi Coverage Mapper. [online]. [cit. 2016-04-01]. Dostupné z: http://play.google.com/store/apps/details?id=pl.ntek.wcm

[6] Wifi Analyzer. [online]. [cit. 2016-04-01]. Dostupné z: http://play.google.com/store/apps/details?id= com.farproc.wifi.analyzer

[7] Speedtest.net. [online]. [cit. 2016-04-01]. Dostupné z: http://play.google.com/store/apps/details?id=org.zwanoo.android.speedtest

[8] MikroTik documentation [online]. Riga: MikroTik, 2008 [cit. 2016-04-01]. Dostupné z: http://wiki.mikrotik.com/wiki/Manual:TOC

[9] Protokoly tunelového propojení VPN. TechNet [online]. Radmong, Washington, USA: Microsoft, 2016 [cit. 2016-04-01]. Dostupné z: https://technet.microsoft.com/cs-cz/library/cc771298%28v=ws.10%2.aspx

[10] OpenVPN. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2015 [cit. 2016-04-09]. Dostupné z: https://cs.wikipedia.org/wiki/OpenVPN

[11] Nagios. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2015 [cit. 2016-04-01]. Dostupné z: https://cs.wikipedia.org/wiki/Nagios

[12] ELLINGWOOD, Justin. An Introduction to SNMP (Simple Network Management Protocol). In: Digital Ocean [online]. New York: Digital Ocean, 2014 [cit. 2016-04-01]. Dostupné z: https://www.digitalocean.com/community/tutorials/an-introduction-to-snmp-simple-network-management-protocol

[13] Check_cciss - HP and Compaq Smart Array Hardware status. Nagios [online]. 2013 [cit. 2016-04-01]. Dostupné z: https://exchange.nagios.org/directory/Plugins/Hardware/Storage-Systems/RAID-Controllers/check_cciss--2D-HP-and-Compaq-Smart-Array-Hardware-Status/details